

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 July 2000 (07.07.00)	
International application No. PCT/AU99/01096	Applicant's or agent's file reference 2241543
International filing date (day/month/year) 08 December 1999 (08.12.99)	Priority date (day/month/year) 08 December 1998 (08.12.98)
Applicant MANGER, James, Howard et al	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:14 June 2000 (14.06.00)☐ in a notice effecting later election filed with the International Bureau on:2. The election ☒ was☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Manu Berrod Telephone No.: (41-22) 338.83.38
---	---

PATENT COOPERATION TREATY

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:
WEBBER, David, Brian
Davies, Collison Cave
1 Little Collins Street
Melbourne, VIC 3000
AUSTRALIE

TUESDAY, 27 JUN 2000

Date of mailing (day/month/year) 15 June 2000 (15.06.00)		IMPORTANT NOTICE	
Applicant's or agent's file reference 2241543			
International application No. PCT/AU99/01096	International filing date (day/month/year) 08 December 1999 (08.12.99)	Priority date (day/month/year) 08 December 1998 (08.12.98)	
Applicant TELSTRA R & D MANAGEMENT PTY. LTD. et al			

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
AU,CN,JP,KP,KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,GE,
GH,GM,HR,HU,ID,IL,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,NZ,
OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
15 June 2000 (15.06.00) under No. WO 00/35141

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---



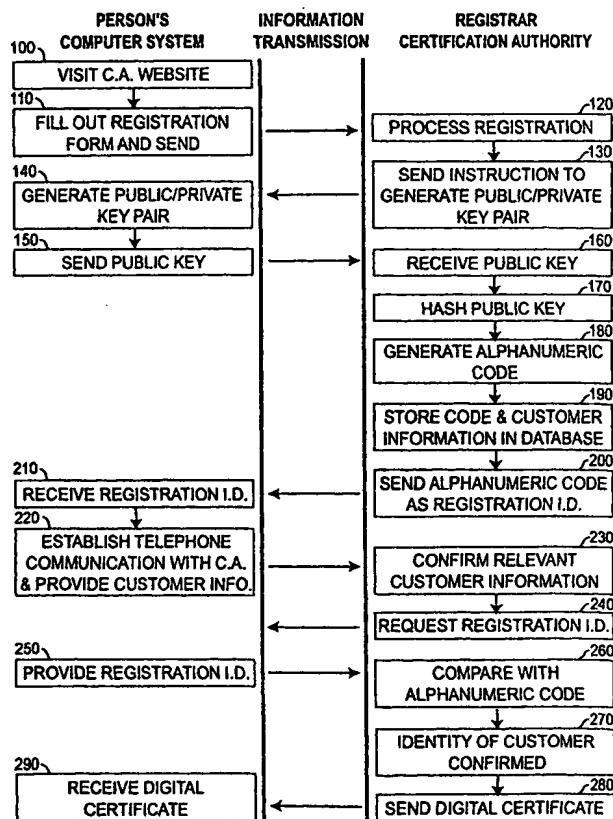
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 9/30		A1	(11) International Publication Number: WO 00/35141
			(43) International Publication Date: 15 June 2000 (15.06.00)
(21) International Application Number: PCT/AU99/01096 (22) International Filing Date: 8 December 1999 (08.12.99) (30) Priority Data: PP 7570 8 December 1998 (08.12.98) AU (71) Applicant (for all designated States except US): TELSTRA R & D MANAGEMENT PTY. LTD. [AU/AU]; 255 Elizabeth Street, Sydney, NSW 2000 (AU). (72) Inventors; and (75) Inventors/Applicants (for US only): MANGER, James, Howard [AU/AU]; Flat 6, 623 Drummond Street, Carlton North, VIC 3054 (AU). ZUK, Edward, Andrew [AU/AU]; 1 Heaton Avenue, Elwood, VIC 3184 (AU). (74) Agent: WEBBER, David, Brian; Davies, Collison Cave, 1 Little Collins Street, Melbourne, VIC 3000 (AU).		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published With international search report.	

(54) Title: A CERTIFICATION METHOD

(57) Abstract

A certification method, system and program which involve processing a public key of a public/private key pair generated by a system of a person, to generate a communicable code representative of the public key. The person is identified by having the person convey the communicable code, and a digital certificate is generated including the public key and identifying information of the person. The certificate binds the public key and the identifying information. The communicable code is a limited character string, which may be generated using a secure one-way hash function.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU 99/01096

A. CLASSIFICATION OF SUBJECT MATTER					
Int Cl ⁷ : H04L 9/30					
According to International Patent Classification (IPC) or to both national classification and IPC					
B. FIELDS SEARCHED					
Minimum documentation searched (classification system followed by classification symbols) IPC: H04L 9/-					
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched AU: IPC as above					
Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) WPAT JAPIO					
C. DOCUMENTS CONSIDERED TO BE RELEVANT					
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.			
X	US 5796833 A (CHEN et al) 18 August 1998 Whole document	1-44			
A	WO 98/25375 A1 (V-ONE CORPORATION) 11 June 1998 Whole document	1-44			
A	US 5664017 (GRESSEL et al) 2 September 1997 Whole document	1-44			
<div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> Further documents are listed in the continuation of Box C <input checked="" type="checkbox"/> See patent family annex </div>					
<table style="width: 100%; border: none;"> <tr> <td style="width: 33%; vertical-align: top;"> <p>* Special categories of cited documents:</p> <p>"A" Document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> </td> <td style="width: 33%; vertical-align: top;"> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p> </td> <td style="width: 33%;"></td> </tr> </table>			<p>* Special categories of cited documents:</p> <p>"A" Document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>	
<p>* Special categories of cited documents:</p> <p>"A" Document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier application or patent but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>				
Date of the actual completion of the international search 07 February 2000		Date of mailing of the international search report 11 FEB 2000			
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No.: (02) 6285 3929		Authorized officer SUSHIL AGGARWAL Telephone No.: (02) 6283 2192			

Information on patent family members

PCT/AU 99/01096

Patent Document Cited in Search Report				Patent Family Member	
WO	9825375	AU	55881/98	US	5784463
US	5664017	IL	113375	US	5852665

PCT
INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Article 36 and Rule 70)

REC'D 20 FEB 2001

WIPO

PCT

Applicant's or agent's file reference 2241543/	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416).
International application No. PCT/AU99/01096	International filing date (<i>day/month/year</i>) 08 December 1999	Priority Date (<i>day/month/year</i>) 08 December 1998
International Patent Classification (IPC) or national classification and IPC Int. Cl.⁷ H04L 9/30		
Applicant 1. TELSTRA R & D MANAGEMENT PTY. LTD. et al		

1.	This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2.	This REPORT consists of a total of 4 sheets, including this cover sheet. <input type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of sheet(s).
3.	This report contains indications relating to the following items: I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application

Date of submission of the demand 14 June 2000	Date of completion of the report 07 February 2001
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer MR MANISH RAJ Telephone No. (02) 6283 2175

I. Basis of the report

1. With regard to the elements of the international application:*

- ☒ the international application as originally filed.
- ☐ the description, pages , as originally filed,
 pages , filed with the demand,
 pages , received on with the letter of .
- ☐ the claims, pages , as originally filed,
 pages , as amended (together with any statement) under Article 19,
 pages , filed with the demand,
 pages , received on with the letter of .
- ☐ the drawings, pages , as originally filed,
 pages , filed with the demand,
 pages , received on with the letter of .
- ☐ the sequence listing part of the description:
 pages , as originally filed
 pages , filed with the demand
 pages , received on with the letter of .

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, was on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the — international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/fig

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-44	YES
	Claims	NO
Inventive step (IS)	Claims 1-44	YES
	Claims	NO
Industrial applicability (IA)	Claims 1-44	YES
	Claims	NO

2. Citations and explanations (Rule 70.7)

None of the prior art documents discloses a certification method which involves generating a communicable code from a public/private key generated by a system of a person, sending said code to said system of said person and identifying said person by having said person convey said communicable code.

The claims meet the criteria as set in out in PCT Article 33(2)-(4).

US 5796833 as cited in the International Search report is considered to be an "A" document.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. In Claim 1, it is not clear as to how the person obtains the communicable code. A similar comment also applies to claims 14, 27, 40 and 44.

2. In Claim 40, it is not clear as to where "a public/private key" pair is generated.

A similar comment also applies to claim 44.

3. In Claim 44, it is not clear as to how "identifying information of a person" is obtained.